

UN RASTREADOR EN TU BOLSILLO

Análisis del sistema de registro de celulares en Colombia

Por: Juan Diego Castañeda

Fundación Karisma

Julio 2017

Fundación Karisma

Bogotá, Colombia
2017

En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean *documentos accesibles*, eso quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas puedan leer, incluidas aquellas que tienen algún tipo de discapacidad visual o de dificultad para la lectura y comprensión.

Más información sobre documentos accesibles en:
http://www.documentoaccesible.com/#que-es

Este documento hace parte de la campaña No más celus vigilados, un proyecto de Fundación Karisma sobre el sistema de registro de celulares en Colombia. La versión digital de Un rastreador en tu bolsillo está disponible en la web de la campaña: http://www.karisma.org.co/nomascelusvigilados

Escrito por:
Juan Diego Castañeda

Revisión:
Carolina Botero
Amalia Toledo

Coordinación editorial:
Laura Rojas Aponte
Camila Barajas Salej

Portada y gráficos:
Mauricio Isaza

Diagramación:
Rubén Urriago

Informe realizado gracias al apoyo de Privacy International
(https://www.privacyinternational.org)

• Índice •

Abreviaturas **5**

Introducción **7**

Descripción de los elementos básicos del sistema de registro de celulares 10

IMEI 10

Bases de datos 11

Base de datos operativa 11

Base de datos administrativa 13

Procedimiento de verificación de IMEI 15

Ciclos de verificación de IMEI irregulares 17

Información analizada para la verificación 17

Control 18

Análisis del sistema de registro de celulares en Colombia **19**

Problemas asociados a las bases de datos del sistema de registro de celulares 20

Cada IMEI está atado a una persona 20

Acceso de autoridades 22

Escenarios problemáticos 24

Problemas derivados del procedimiento de verificación de IMEI 25

Vigilancia de las comunicaciones. 25

Retención y acceso a la información de las comunicaciones celulares 26

Metadatos de las comunicaciones: recopilación y entrega de CDR 28

Protecciones internas a las comunicaciones. 30

Problemas del sistema en general 34

El sistema está en manos de terceros 34

No puede ser la única solución. 35

La BD positiva y el proceso de verificación no sirven para combatir el hurto 37

Conclusiones. 39

Recomendaciones 41

A la Comisión de Regulación de Comunicaciones 41

Al Ministerio TIC. 42

A los operadores de telefonía móvil. 43

A la Autoridad de Protección de Datos. 44

• Abreviaturas •

ABD – Administrador de la base de datos. Persona jurídica encargada de la Administración de la BDA en la cual se almacena la información asociada a equipos terminales móviles. Actualmente está en cabeza de la empresa El Corte Inglés.

CRC – Comisión de Regulación de las Comunicaciones.

BDA – Base de datos administrativa. Bases de datos centralizadas, tanto positiva como negativa, administrada por el ABD, la cual contiene datos que provienen de las BDO de cada operador.

BDO – Base de datos operativa. Base de los IMEI autorizados para funcionar (positiva) y los no autorizados a funcionar (negativa) administrada por cada operador.

BDA/BDO negativa – Base de datos administrativa/base de datos operativa negativa. Bases de datos que almacenan la relación de los IMEI y demás información necesaria de todos los equipos terminales móviles que han sido reportados como robados o perdidos tanto en Colombia como en el exterior y que, por lo tanto, están inhabilitados para operar en las redes de telecomunicaciones móviles del país.

BDA/BDO positiva – Base de datos administrativa/base de datos operativa positiva. Bases de datos que almacena, la relación de los IMEI de los equipos terminales móviles ingresados, fabricados o ensamblados legalmente en el país. Cada IMEI registrado en esta base de datos deberá estar asociado con la información del propietario del equipo terminal móvil o del propietario autorizado por éste.

CDR – Call/Charge Detail Record. Información de los detalles de llamadas y uso de datos, como tipo de llamada, tiempo, duración, origen y destino. Los CDR pueden ser usados para el control de la red, contabilidad y propósitos de facturación.

ETM – Equipo Terminal Móvil. Equipo electrónico que posea un identificador internacional único (el IMEI), por medio del cual el usuario accede a las redes de comunicaciones móviles. Se trata de celular, smartphone, ciertas tabletas, etc.

GSMA – GSM Association. Asociación mundial que representa los intereses de la industria de la telefonía móvil. Asigna los IMEI válidos y maneja una base de datos negativa mundial de IMEI.

ICCID – Integrated Circuit Card Identifier. Número serial único de la tarjeta SIM, guardado en ella y grabado físicamente.

IMEI – International Mobile station Equipment Identity. Código de 15 dígitos pregrabado en los equipos terminales móviles que lo identifica de manera específica al nivel mundial. Tanto la identificación como el bloqueo de un terminal móvil está basada en este número.

IMSI – International Mobile Subscriber Identity. Código Internacional del abonado o suscriptor móvil, es un código único que identifica a cada abonado del teléfono móvil en el estándar GSM y en redes de nueva generación (GPRS, Edge, 3G y 4G), y que adicionalmente permite su identificación en la red. El código se encuentra grabado en la tarjeta SIM.

Ministerio TIC – Ministerio de las tecnologías de la información y las comunicaciones.

MSISDN – Mobile Subscriber Integrated Services Digital Number. Estación Móvil de la Red Digital de Servicios Integrados (RDSI). Número telefónico de una tarjeta SIM en el sistema GSM y UMTS, o número de identificación único de un suscriptor.

PRSTM – Proveedor de Redes y Servicios de Telecomunicaciones Móviles. Empresas que proveen acceso a las redes móviles tales como Claro, ETB, etc.

SIM – Subscriber identification (or Identity) Module o Módulo de identidad del abonado. Dispositivo electrónico que almacena información técnica de la red, así como también la información de identificación de una cuenta de servicios de telecomunicaciones. Se presenta en general como tarjeta chip de contacto. Concretamente, contiene el Mobile Country Code (MCC), Mobile Network Code (MNC) y el Mobile Subscription Identification Number (MSIN).

SIC – Superintendencia de Industria y Comercio.

TAC – Type Allocation Code. Código que la GSMA asigna a los fabricantes de celulares y que permite identificar la marca, el modelo y otras características del equipo.[1] Este código constituye los primeros 8 dígitos del IMEI.

TIC – Tecnologías de la Información y las Comunicaciones.

[1] Definición adaptada de la Resolución CRC 3128 del 7 de septiembre de 2011, artículo 2.

• Introducción •

Cuando un celular es robado, en principio, solo basta con cambiarle la SIM para que funcione, lo que hace del robo de celulares una de las actividades ilegales más lucrativas en el país. Para contrarrestar este flagelo, el gobierno colombiano decidió aprovechar las características técnicas de los celulares con el objetivo de que, al reportar el robo o la pérdida de un aparato, este ya no pueda funcionar en las redes sin importar qué SIM u operador use.

A diferencia de lo que sucede con los radioteléfonos o *walkie-talkies*, para que un celular funcione debe probar a la red de telefonía que está autorizada para hacer y recibir llamadas, y para enviar y recibir datos. Básicamente, la función de la SIM *card* es permitir esa comprobación: hacerle saber a la red cuál es la cuenta a la que se le debe cargar el servicio, o si tiene suficiente saldo de voz o de datos para usar el celular. Sin embargo, el intercambio de información entre el celular y la red no solo involucra la SIM, también se puede enviar y recibir información sobre el celular en sí mismo.

Este sistema de registro de celulares se basa en el hecho de que la red pueda identificar cuál es el aparato, no solo la SIM, que está solicitando conexión. Esta identificación de los celulares se puede hacer a través del IMEI, que es un número único, asignado por la GSMA a los fabricantes de celulares, para cada aparato e impreso físicamente. Este identificador queda guardado dentro de la memoria interna del dispositivo.

La idea del sistema de registro de celulares es usar el IMEI para identificar los celulares reportados como robados o perdidos para impedirles el acceso a la red. De esta forma, se crean incentivos para disuadir el robo de celulares. El bloqueo de celulares a partir del IMEI no es exclusivo de Colombia. En otras partes del mundo existen regímenes que impiden el funcionamiento en la red de telefonía a celulares reportados como robados.[2] Sin embargo, el sistema creado en Colombia

---

[2] *Véase*, por ejemplo, en Estados Unidos: Federal Communications Commision. (s.f.). *Proteja su teléfono inteligente* [blog post]. Disponible en https://www.fcc.gov/consumers/guides/proteja-su-telefono-inteligente; y en Reino Unido: Ofcom. (2015, 13 de junio). *Lost or stolen phon*e. Disponible en https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/safety-and-security/lost-or-stolen-phone.

va mucho más allá. Para empezar, en el país existen dos listas o bases de datos: una negativa, en donde quedan recogidos los celulares reportados robados, y una positiva, que contiene aquellos dispositivos autorizados a funcionar.

Seguidamente, el sistema colombiano contra el robo de celulares obliga a los operadores a hacer una constante revisión en las dos bases de datos. Además, deben verificar periódicamente los dispositivos que funcionan en sus redes telefónicas para identificar y evitar que funcionen aquellos celulares reportados como robados o perdidos. Y para que este sistema opere, requiere de una colosal cantidad de datos personales que deben recolectarse y que incluso requieren ser cruzados entre sí.

Este sistema es complejo y ha sido creado por varias normas. La primera, que creó el sistema, es una norma elaborada por el Ministerio TIC en mayo de 2001.[3] Un mes más tarde el Congreso encargó a la CRC establecer las condiciones de funcionamiento de estas bases de datos.[4] Finalmente, la CRC expidió una resolución que ha sido ampliada y modificada en múltiples ocasiones, la última de ellas en octubre de 2016.[5] Es importante establecer que el presente documento explica la regulación en el estado en que se encontraba a diciembre de 2016.

El sistema se refiere a toda clase de aparatos, por ejemplo, celulares, tablets o lectores de libros electrónicos, que acepten una SIM *card*, que usen la red móvil y que, por tanto, deben tener IMEI. La reglamentación se refiere a ETM en general. Sin embargo, para facilitar la lectura en este texto simplemente hablaremos de celulares.

Para aclarar algunas partes del sistema, hemos usado los documentos que produjo la CRC en el proceso regulatorio y los comentarios de los operadores de telefonía celular presentados durante ese mismo proceso. En ese sentido, aunque haya diferencias en la implementación, se trata de evaluar la regulación tal y como está escrita, independientemente de cómo la interpretan quienes hoy participan en el sistema.

El documento está estructurado en dos partes. En la primera, describimos los elementos básicos del sistema: las bases de datos y el procedimiento de verificación. En la segunda, hacemos el análisis crítico del sistema, así: (1) las bases de datos y el problema de la unión entre IMEI y datos personales; (2) el procedimiento de verificación y el contexto de la vigilancia de las comunicaciones en Colombia; y (3) el sistema en general y las dificultades que plantea el hecho de que pretende ser la principal solución al problema del robo de celulares.

---

[3] Decreto 1630 de 19 de mayo de 2011 .

[4] Ley 1453 de 24 de junio de 2011, artículo 106.

[5] Resolución CRC 3128 de 7 de septiembre de 2011. Disponible en https://www.crcom.gov.co/recursos_user/Normatividad/Normas_Actualizadas/Res_3128_11_Act_5038_16.pdf.

Como se verá, el sistema de registro de celulares tal como está implica graves riesgos hacia los derechos a la intimidad y a la libertad de expresión en la medida que obliga a identificar más allá de lo necesario a las personas dueñas de teléfonos celulares, además de recopilar información sobre sus comunicaciones, conocidos como metadatos. Aún bajo estos estrictos controles a los teléfonos celulares, los problemas que pretende solucionar el sistema persisten, así como los riesgos a los derechos fundamentales de las personas usuarias de estos aparatos.

Existen otras razones por las que un control a la venta de celulares como el impuesto no es conveniente, especialmente para el derecho al acceso a la tecnología y a internet, para el derecho a la participación de la vida cultural y de los avances de la ciencia y la tecnología o el derecho a la educación.[6] Sin embargo, el enfoque de este documento es el riesgo al ejercicio de los derechos a la intimidad y a la libertad de expresión por efecto del registro de información personal en relación con cada celular, así como la recopilación de metadatos de las comunicaciones en el contexto de la vigilancia para investigaciones penales y actividades de inteligencia.

Al final se formulan recomendaciones dirigidas a las principales autoridades que han diseñado, promovido y defendido el actual sistema. El objetivo de estas recomendaciones es evidenciar que hay formas de cambiar el sistema actual y hay alternativas que, aunque pueden tener los mismos efectos sobre el robo de celulares, no afectan injustificadamente los derechos a la intimidad y a la libertad de expresión.

---

[6] Instituto de Tecnología & Sociedad do Río y Access. (2015). *Connectivity at Risk: Study on the impact of blocking uncertified mobile devices in Brazil*. Disponible en https://www.accessnow.org/cms/assets/uploads/archive/docs/ITS_Report_English_Final_1.pdf.

Descripción de los elementos básicos del sistema de registro de celulares

El sistema de registro tiene dos componentes básicos. Uno, las bases de datos de IMEI y, dos, el procedimiento de verificación. Antes de explicar en detalle cada uno, explicaremos qué es el IMEI y por qué es el centro del sistema.

IMEI

La identidad internacional de equipo terminal móvil, IMEI en inglés, es un número único que identifica a cada celular. Este número es asignado por la Asociación GSM (GSMA) desde el año 2000 y está formado por 15 dígitos.[7] Los primeros 8 corresponden, en general, al código del modelo del celular. Este conjunto de 8 dígitos es conocido como TAC (Type Allocation Code). Los siguientes 6 dígitos son el número único del equipo. El último es un dígito de verificación.[8]

Los operadores pueden controlar qué celulares pueden usar sus redes a través de un dispositivo conocido como registro de identidad de equipos (EIR, en inglés).

[7] Antes del año 2000, los fabricantes obtenían la identificación del equipo ante las autoridades nacionales en Europa. Al ser abolida esta obligación, la asignación de códigos de certificación (type allocation codes) pasó a ser realizada por la GSMA. *Véase* GSMA. (2017, 24 de febrero). *IMEI Allocation and Approval Process*. Version 11.0.

[8] Por ejemplo, un iPhone 6s tiene un IMEI 35541607XXXXXX4, siendo 541607 el código que identifica el modelo del celular. Los dígitos X son el número específico de cada iPhone 6s.

Bases de datos

El sistema de bloqueo de celulares está estructurado alrededor de dos listas, o bases de datos, de IMEI: una positiva y otra negativa. En la negativa entran los IMEI que deben bloquearse. En la positiva los que están autorizados para funcionar en las redes de los operadores.

Esta lista tiene dos niveles: el de cada operador y el centralizado. En el primer nivel, cada operador tiene una base de datos negativa y positiva. Estas son las llamadas bases de datos operativas (BDO). Hasta este punto, si una persona reporta a su operador que su celular fue robado, el operador bloquea el IMEI *en sus redes*. Sin embargo, esto no significa que el celular está bloqueado en las redes de otros operadores. Por ejemplo, un celular que solo está en la base de datos negativa de Tigo, podría funcionar en Movistar o Claro. Para evitar este problema, todos los operadores deben anotar en una base de datos compartida los IMEI que han sido reportados. Este es el segundo nivel, el de las bases de datos centralizadas, llamadas en la regulación bases de datos administrativas (BDA). Por este medio, todos los operadores conocen todos los IMEI reportados. Esta es la BDA negativa.

Base de datos operativa

La regulación llama BDO a aquellas que tienen los operadores y en las que registran IMEI para permitir o impedir que funcionen en la red. Los primeros se registran en la BDO positiva, y los segundos en la BDO negativa.

BDO Negativa

Esta base de datos almacena los IMEI de celulares reportados como perdidos o robados y que, por tanto, no pueden funcionar en las redes de los operadores.

En concreto, estas bases de datos tienen los IMEI de equipos:[9]

- Reportados a cualquier operador.
- Bloqueados por no estar en la base de datos positiva.
- Bloqueados como resultado del procedimiento de verificación.

[9] Resolución CRC 3128 de 2011, artículo 7, inciso 2a9.

- Reportados desde bases de datos centralizadas (BDA) de otros países con los que haya intercambio de esta información.[10]
- Reportados como robados o perdidos según la GSMA.
- Irregulares (duplicados, inválidos, no homologados) a partir del momento en que la CRC establece el bloqueo de esos IMEI.

Los IMEI deben conservarse por 3 años cuando son reportados en Colombia, y 1 año los reportados provenientes del exterior.[11]

BDO Positiva

Esta base contiene los IMEI autorizados para funcionar en las redes de los operadores del país. La forma en la que se registra el IMEI en esta base depende de la modalidad del contrato que tenga la persona o del hecho de haber sido importado el celular al país. En la **modalidad pospago**, el operador es quien hace el registro. La regulación requiere que se asocien al IMEI los datos de identificación de la persona y que el operador compruebe su identidad.[12]

En la **modalidad prepago**, el operador debe disponer en sus esquemas de atención al cliente de la opción de "registrar el equipo". En concreto, tiene que:[13]

- Verificar la tenencia del celular a través de uno de dos métodos: (1) con información del cliente en el sistema del operador, verificar esa asociación entre celulares y cliente; o (2) enviar un mensaje de texto con un código de verificación y solicitarlo en el proceso de activación en línea.
- Identificar el IMEI y revisar que sea válido.
- Solicitar los "nombres, apellidos, tipo de documento, número de identificación, dirección y teléfono de contacto" de quien quiere hacer el registro.
- Comprobar la identidad de la persona.

Para la importación, el fabricante es quien reporta los IMEI que está importando.

La norma no dice nada sobre el tiempo de conservación pero se entiende que los operadores deben conservar esta información perpetuamente, lo que implica también la conservación de los datos personales necesarios para el registro.

---

[10] La Decisión Andina 786 de 24 de abril 2013 obliga a algo similar al establecer que los operadores en cada país deben compartir la información de los IMEI reportados, a través del uso del sistema de la GSMA.

[11] Resolución CRC 3128 de 2011, artículo 7.

[12] Ibíd., artículo 7a, inciso 1.

[13] Ibíd., artículo 7a, literales a-f.

Base de datos administrativa

Como se menciona antes, bloquear un IMEI reportado en las redes de un operador no es suficiente pues bastaría con cambiar de operador para que el celular reportado vuelva a funcionar. Para que no funcione en ninguna red, es necesario que los operadores compartan la misma lista de IMEI reportados. Esta es la función de la BDA, que recoge las bases de datos positivas y negativas de todos los operadores, pero solo sincroniza entre todos los operadores las bases de datos negativas.

Como pasa con las BDO, la BDA está compuesta por las bases de datos positiva y negativa.

BDA Negativa

La BDA negativa, aparte de contener los registros recogidos en las BDO negativa, incorpora los reportes que reciba de las bases de datos centralizadas de otros países — es decir, las BDA de otros países— y las que envíe la GSMA.

Registro histórico de la base administrativa negativa: Después del tiempo mínimo de permanencia en la BDA negativa, los IMEI que estuvieron en ella deben ser retirados de las BDO y deben quedar conservados en un registro. El administrador de la BDA debe remitirlos cada 6 meses a los operadores para verificar que no estén generando tráfico en la red. Si están generando tráfico, el operador debe bloquear el IMEI, enviarlo a la BDA y notificar a la CRC.[14]

BDA Positiva

Esta base de datos recogerá los IMEI importados legalmente y los registrados en las BDO positivas. La actualización de los datos de esta base de datos es la misma que se explica para el caso de la BDO positiva.

Los operadores deben mantener actualizada la BDO y sincronizarlas con la BDA.

[14] Ibíd., artículo 7, párr. 1.

CADA OPERADOR TIENE DOS BASES DE DATOS LLAMADAS "BASES DE DATOS OPERATIVAS" (BDO)

BD Negativa

IMEI

- Reportados por robo o pérdida
- No registrados
- Detectados en el procedimiento de verificación

BD Positiva

Contiene por cada celular:

IMEI

MSISDN
Número de teléfono

IMSI

Junto con información personal del propietario del celular:

- Nombres y apellidos.
- Documento de identificación.
- Dirección y teléfono de contacto.

Otra base de datos, llamada "Base de Datos Administrativa" (BDA), **recoge** la información de las BDO positivas y **sincroniza** las BDO negativas para que todos los operadores tengan al día la lista de IMEI que deben bloquear.

BD Administrativa

BD Negativa

BD Positiva

Las autoridades administrativas, policivas y judiciales pueden acceder a la BDA.

Procedimiento de verificación de IMEI

El registro de celulares en las bases de datos que hemos descrito antes se complementa con un método de verificación de cada uno de los celulares que han estado activos en las redes móviles. Esta verificación busca que solo operen en Colombia celulares homologados, con un IMEI legítimo y que estén registrados en la BDA positiva.[15]

Para que solo los celulares homologados y registrados en la BDA positiva puedan operar en las redes móviles, la CRC creó un mecanismo para detectar y verificar IMEI irregulares que hagan uso de la red. Se entienden como irregulares los IMEI cuando son:

- **Inválidos:** IMEI cuyo TAC no está en la lista de la GSMA o en la de marcas y modelos homologados por la CRC.
- **Sin formato:** IMEI que no son consistentes con estándares de la industria (3GPP, TS 22.2016 y TS 23.003), cuya longitud es equivocada o que tienen caracteres alfabéticos.
- **No homologados:** IMEI cuyo TAC no está en la lista de marcas y modelos homologados por la CRC.
- **No registrados:** IMEI que no aparecen en la BDA positiva.
- **Duplicados:** Ya que es posible reescribir el IMEI de un celular, un celular puede tener un IMEI inválido o sin formato, pero también puede tener un IMEI que ya tiene otro equipo, también llamado IMEI clonado.[16] Cuando a un celular robado o perdido se le reasigna un IMEI que está en la base de datos positiva, la red detectará actividad proveniente de un celular legítimo, por lo que le prestará el servicio. Por eso, la CRC obliga a los operadores a detectar casos donde posiblemente dos celulares estén usando el mismo IMEI. Estos casos son:
  - Cuando un mismo IMEI está haciendo dos llamadas al tiempo, pero registra diferente IMSI. Este es el criterio de simultaneidad de las llamadas.
  - Cuando es imposible que desde un mismo IMEI se hayan hecho llamadas a una distancia imposible de recorrer en un cierto tiempo. Por ejemplo, cuando un mismo IMEI con diferentes IMSI hacen llamadas en menos de 10 minutos, conectándose a estaciones que están a más de 25 kilómetros de distancia.[17]

Los operadores deben tomar los IMEI que hayan registrado actividad en la red de telefonía móvil y evaluar su situación según el tipo de irregularidad. Los IMEI que sean detectados en este filtro recibirán el tratamiento correspondiente de acuerdo a su problema. Los que no sean detectados, vuelven a ser analizados al día siguiente.[18]

---

[15] Resolución CRC 4813 de 2015, artículo 4.

[16] La alteración del IMEI es un delito. Ley 1453 de 24 de junio de 2011, artículo 105.

[17] El artículo 10b.1., numeral v de la Resolución CRC 3128 de 7 de septiembre de 2011 muestra una tabla que indica los parámetros de tiempo y distancia para determinar la existencia de un conflicto que debe ser detectado. El mínimo es 2 minutos y 5 kilómetros de distancia. El máximo es 60 minutos y 150 kilómetros de distancia.

[18] CRC. (2016). *Revisión de las condiciones y criterios para la identificación de equipos terminales móviles: Etapa de control.*

VERIFICACIÓN DE DUPLICADOS

El proceso de verificación busca IMEI irregulares.
Uno de ellos es el **IMEI duplicado**. Éste ocurre en dos casos:

SIMULTANEIDAD DE LLAMADAS

Se produce cuando diferentes líneas (IMSI) con un mismo IMEI hacen llamadas al mismo tiempo.

CONFLICTO TIEMPO-DISTANCIA

Se produce cuando diferentes líneas (IMSI) con un mismo IMEI hacen llamadas a cierta distancia en menos de cierto tiempo.

"Se detecta un duplicado cuando se encuentra que diferentes líneas, pero un mismo IMEI hizo llamadas desde puntos separados por 10 km en menos de 4 minutos".

TIEMPO	DISTANCIA
0,8 min	2 Km
4 min	10 Km
10 min	25 Km
60 min	150 Km

Para que este análisis sea posible se requiere que:

- Los operadores recopilen y analicen los metadatos de las comunicaciones.
- Los operadores informen sobre la ubicación geográfica de sus torres.

LOS METADATOS

Son información que produce automáticamente la tecnología móvil e indican:

- Cuándo inició y cuándo terminó la llamada.
- Dónde inició la llamada y dónde terminó.
- Qué IMEI hizo la llamada.
-Qué IMSI hizo la llamada.

Ciclos de verificación de IMEI irregulares

Los operadores deben analizar la información de sus redes diariamente y encontrar cuáles IMEI cumplen alguno de los criterios anteriores y, por tanto, son irregulares. Paralelamente, los operadores deben entregar la información de sus redes para que detecte los IMEI duplicados entre operadores según el criterio que ya se describió. La regulación llama al análisis que hace cada operador en su red "ciclo intra red". Al análisis que hace un tercero para encontrar duplicados entre operadores lo llama "ciclo inter red".[19]

Información analizada para la verificación

La detección de IMEI irregulares hace uso de la información que produce automáticamente la telefonía celular. Esta es información sobre qué número hace la llamada, qué dispositivo la hace (identificando IMEI, IMSI, MSISDN, etc.), qué número la recibe, cuánto tiempo dura, desde dónde se realiza, entre otros. Este registro es conocido como CDR. En resumen, esta información consiste en:[20]

- IMEI
- IMSI
- Tipo de llamada: originada o terminada
- Fecha y hora de inicio y fin de cada llamada
- Código que identifica desde dónde se inicio y terminó la llamada

Para el ciclo inter red, los operadores deben entregar a quien esté encargado del análisis la lista de IMEI que identificaron como duplicados y de IMEI en regla, es decir, que no son irregulares. Si se requiere, aunque no sea claro en qué condiciones, el encargado del análisis entre redes puede solicitar la siguiente información, discriminando llamadas originadas y terminadas de los IMEI duplicados:

- Hora de inicio y fin de la llamada
- IMEI
- IMSI
- Identidad de la celda
- Código de localización de área de inicio y fin de cada llamada

[19] Resolución CRC 3128 de 7 de septiembre de 2011, artículos 10a y 10b.

[20] Ibíd., artículo 10a.9, literal b.

Adicionalmente, la CRC puede pedir otra información contenida en los CDR en caso de considerarlo necesario. Toda esta información, que se conoce internacionalmente como los metadatos de las comunicaciones, debe ser enviada a la CRC.[21]

Como se mencionó antes, ya que para detectar un IMEI duplicado la CRC estableció en uno de los casos la necesidad de analizar parámetros de tiempo y distancia, se exige a los operadores que entreguen la información de la ubicación geográfica de sus estaciones al encargado del análisis entre redes.[22]

Control

Las consecuencias que siguen a la detección de un IMEI irregular varían según cada caso y explicarlas en detalle está por fuera de los objetivos de este documento. Sin embargo, la idea del sistema es que todo IMEI irregular sea bloqueado.

Adicionalmente, vale la pena hacer referencia al caso específico de los IMEI duplicados y su medida de control. Cuando se detecta un IMEI duplicado, el operador debe notificar a la persona usuaria (o usuarias) que debe presentar los soportes de la compra del celular o de lo contrario este será bloqueado. En caso de que la persona, efectivamente, presente los soportes y realice el trámite correspondiente, el operador debe registrar la pareja IMEI-IMSI. Esto quiere decir que el operador autorizará el funcionamiento de ese celular en su red solo con un número específico, que es el que provee la persona que logra probar que es dueña legítima del celular. Los IMEI duplicados no asociados a un IMSI serán registrados en la BDA negativa, pero no se eliminará el registro de la identificación en la BDA positiva.[23]

[21] Ibíd., artículo 10a.9, literales b y d.

[22] Ibíd., artículo 10a, numeral 10a.2.

[23] Ibíd., artículo 10d, literal c, numerales c.7 a c.11.

Análisis del sistema de registro de celulares en Colombia

En el capítulo anterior se describen los elementos básicos del sistema de registro de celulares y el procedimiento de verificación. Además, se da el contexto para el análisis que haremos a continuación. Algunos elementos del sistema han sido omitidos en la descripción porque serán mencionados en este capítulo junto con los problemas que el sistema plantea para los derechos a la intimidad y a la libertad de expresión. Justamente, el marco del análisis es el del Derecho Internacional de los Derechos Humanos, tanto del sistema universal como del interamericano, como también de la Constitución Política. Así mismo, haremos referencia a los *Principios Internacionales sobre la aplicación de los Derechos Humanos a la vigilancia de las comunicaciones*.[24]

Como se ha mencionado, el sistema busca resolver el problema del robo de celulares, pero para hacerlo busca el control total de las comunicaciones de las personas sin analizar debidamente las afectaciones que se producen. Los principales derechos en juego son el derecho a la intimidad y el derecho a la libertad de expresión. El derecho a la intimidad constituye una protección en favor de las personas contra toda "injerencia arbitraria en su vida privada, su familia, su domicilio o su correspondencia".[25] La Constitución colombiana es más específica al proteger las comunicaciones privadas y establecer que solo pueden ser interceptadas por orden judicial y en los casos que lo permita la ley.[26] Por su parte, el derecho a la libertad de expresión protege la posibilidad de recibir y difundir informaciones y opiniones.[27] La relación de este derecho con la existencia de registros y la vigilancia de las comunicaciones se amplía adelante.

Ahora bien, los elementos más problemáticos de este sistema respecto a los derechos a la intimidad y la libertad de expresión tienen que ver, en primer lugar, con cómo se une el registro de información personal de quien posee un celular con el IMEI, IMSI y el número de teléfono y, por otra parte, el acceso irrestricto que tienen diferentes autoridades a esta información.

---

[24] *Principios Internacionales sobre la aplicación de los Derechos Humanos a la vigilancia de las comunicaciones*. (2014, 10 de mayo). Disponible en https://necessaryandproportionate.org/es/necesarios-proporcionados.

[25] *Véase* el artículo 12 de la *Declaración Universal de Derechos Humanos*; el artículo 17(1) del *Pacto Internacional de Derechos Civiles y Políticos*; el artículo 11(2) de la *Convención Americana sobre Derechos Humanos*.

[26] Constitución Política (1991), artículo 15.

[27] *Declaración Universal de Derechos Humanos*, artículo 19; *Pacto Internacional de Derechos Civiles y Políticos*, artículo 19(2); *Convención Americana sobre Derechos Humanos*, artículo 13(1).

El sistema de registro de celulares en Colombia no se limita a las bases de datos, incluye otro nivel de complejidad que es el proceso de verificación ya descrito en la primera parte del documento. Esta verificación también representa importantes retos para los derechos humanos:

- La obligación que se impone a los operadores de recopilar metadatos de las comunicaciones.
- La obligación de entregar esos datos a un tercero y a la CRC.
- La falta de consideración sobre lo que significa ordenar la recopilación de metadatos en el contexto de la vigilancia de las comunicaciones en Colombia.

A esta lista de problemas se agregan otros cuantos que tienen que ver con el sistema en general. Uno de ellos es que la administración del sistema está en manos de terceros. También es necesario evidenciar que su desarrollo ha estado guiado por la pretensión de que el bloqueo de celulares con IMEI reportado como robado sea visto como la solución final a esta compleja cadena de criminalidad.

Este punto del documento y su análisis seguirá este orden: bases de datos, procedimiento de verificación y visión del sistema en general.

Problemas asociados a las bases de datos del sistema de registro de celulares

Cada IMEI está atado a una persona

Como quedó explicado antes, las BDO y BDA positivas no solo contienen los IMEI que pueden funcionar en las redes, sino que asocian al IMEI a otros datos personales sin ninguna necesidad y sin sustento legal. En primer lugar, aparte del IMEI, la BDO positiva debe contener “la información correspondiente a IMEI-IMSI-MSISDN”.[28] Esto quiere decir que no solo se registra el IMEI junto con los datos anteriores, sino que también debería registrarse el número único del suscriptor (IMSI) y el número de teléfono (MSISDN). Esta asociación entre IMEI, IMSI y número de teléfono no aparece ni el decreto ni en la ley.

El Decreto 1630 de 2011 sí señala específicamente que el IMEI de cada celular debe asociarse con el “número de identificación de cada propietario del equipo”.[29] Sin embargo, para la resolución, esto significa asociar al IMEI “nombres, apellidos, tipo de documento, número de identificación, dirección y teléfono de contacto”. Esta información debe ser verificada como se describe a continuación.

---

[28] Resolución CRC 3128 de 2011, artículo 7 inciso 1.

[29] Ibíd., artículo 7.

Comprobación de la identidad

Para las modalidades prepago y pospago, los operadores deben verificar la identidad que provea la persona en "al menos, una de las siguientes fuentes":

- Archivo Nacional de Identificación.
- Registraduría Nacional del Estado Civil.
- Centrales de riesgo crediticio.
- Datos históricos de personas que tenga el operador de la persona usuaria.

Según el Código de Policía que empezó a regir a partir de 2017, activar una línea telefónica o una SIM card sin que la persona haya suministrado al operador sus "datos biográficos" constituyen "comportamientos que afectan la seguridad de las personas" y sus celulares.[30] En caso de incumplimiento, la policía podrá imponer una multa de hasta 32 salarios mínimos y destruir el celular.[31]

Este registro de la información personal junto con el IMEI, IMSI y número de línea a datos personales es problemático. En primer lugar, en el decreto no hay una justificación de la necesidad de cruzar esta información, por lo que esta medida es arbitraria. Además, no es legal, pues la Ley 1453 de 2011 no obliga a hacer esta asociación.

Hasta el momento no es claro por qué es indispensable unir la información personal de quienes contratan servicios de telefonía móvil con los datos de su celular. Al contrario, sí es claro que esta asociación de datos no es efectiva para fines de seguridad y sí constituye una traba ilegítima al derecho a la intimidad y a la libertad de expresión. Más aún, la GSMA reconoce que no existen evidencias de que el registro personal de la *SIM card* ayude a reducir la criminalidad.[32] Países como México, Canadá y Reino Unido han rechazado esta práctica por esa misma razón.[33] Ni el legislador ni el regulador en Colombia han presentado evidencia alguna de la necesidad de registrar no solo la *SIM card*, sino también el celular.

Por otra parte, el Relator Especial de las Naciones Unidas para la libertad de expresión ha señalado que es preocupante que en varios países africanos se están estableciendo bases de datos que relacionan la información de las personas con la *SIM card*, "eliminando la posibilidad del anonimato en las comunicaciones, posibilitando el rastreo de la ubicación y simplificando la vigilancia de las comuni-

---

30 *Código Nacional de Policía y Convivencia*. Ley 1801 de 29 de julio de 2016, artículo 95, numerales 12 y 13.

31 Ibíd., artículo 180.

32 GSMA. (2013). *The mandatory Registration of Prepaid SIM Card Users . A White Paper*. Disponible en http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf.

33 Sobre la posición de la GSMA y el registro de *SIM cards* en otros países, *véase* Ibid.

caciones”.[34] Además, esta información ayuda a crear “perfiles integrales” de las personas. Este tipo de sistemas pueden excluir de la telefonía móvil a quien no pueda o quiera entregar sus datos personales para registrarse.[35]

Tal y como está el sistema de registro en Colombia, detrás de cada IMEI hay una persona. No importa que la persona que usa el celular es la persona que aparece en el registro pues esta circunstancia puede revelar aún más información personal. Así, por ejemplo, las personas menores de edad tendrán su celular registrado a nombre del padre o de la madre o el celular de trabajo de una persona revelará el nombre del representante legal de la empresa dueña del aparato.

Acceso de autoridades

Aunque en Colombia la Constitución protege las comunicaciones de las personas, las reglas que rigen el sistema de registro de celulares permiten el acceso ilegítimo de autoridades a la información que se recoge en las bases de datos. En primer lugar, el Decreto 1630 de 2011, al hablar de la base de datos negativa, obliga al operador a mantener la información actualizada y garantizar “su consulta en línea, registro a registro, por parte de las autoridades administrativas, policivas o judiciales, con observancia de las normas vigentes en materia de protección de datos personales”.[36]

La Resolución 3128 de 2011, por su parte, permite el acceso a las bases de datos administrativas para que “autoridades administrativas [...] así como las autoridades policivas y judiciales” consulten la información “en forma exacta y actualizada, registro a registro”.[37] Uno de los problemas con esta norma es que la resolución excede lo que permite el decreto, ya que este último habla solamente del acceso a la BDO negativa, mientras que la resolución lo convierte en acceso a las BDA, que contiene la información de todos los operadores, tanto de las bases negativas como de las positivas.

Sin embargo, el principal problema es que las autoridades que pueden acceder a la información de las bases de datos de IMEI están definidas de manera ambigua. El Consejo de Estado ha tratado este tema al decidir sobre una acción de nulidad contra el Decreto 1704 de 2012, que obliga a los operadores a colaborar con la interceptación de comunicaciones ordenadas por las autoridades competentes. Este es un caso similar al del registro de celulares, ya que el decreto demandado permitía a la Fiscalía General o “demás autoridades competentes” acceder a los datos de la persona suscriptora de servicios de telefonía. La demanda se dirigió contra

---

[34] Human Rights Council. (2013, 17 de abril). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40, párr. 70. Disponible en http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[35] Ibíd.

[36] Decreto 1630 de 19 de mayo 2011, artículo 6.

[37] Resolución CRC 3128 de 7 de septiembre de 2011, artículo 9.

la expresión "demás autoridades competentes", que el Consejo de Estado declaró nula porque el Gobierno había excedido sus facultades al reglamentar la ley más allá de sus términos. Así, el decreto le habría concedido facultades a autoridades distintas a la Fiscalía cuando la ley y la Constitución era específica al respecto.

El Decreto 1630 de 2011 no está soportado en la Ley 1453 de 2011, pues es anterior a ella. El fundamento, en cambio, lo encuentra en la Ley 1341 de 2009, que faculta al Estado a intervenir en el sector de las TIC para proteger los derechos de las personas y para imponer a los operadores obligaciones por razones de seguridad pública.[38]

Permitir el acceso a "autoridades administrativas, policivas y judiciales" está injustificado, pues no es claro qué autoridades pueden acceder a la información ni por qué motivos. En comparación, cuando la Fiscalía está investigando un delito puede solicitar una búsqueda selectiva de información en bases de datos, pero esta solo la puede ordenar la Fiscalía, la puede llevar a cabo los órganos de policía judicial (el Cuerpo Técnico de Investigación de la Fiscalía, por ejemplo) y debe ser autorizada por un juez de control de garantías.[39] Claramente, la búsqueda de información en las bases de datos que hacen parte del sistema de registro de celulares debería estar sometida a las mismas protecciones. Por otra parte, el sistema no exige condiciones ni motivos para el acceso a las bases de datos.

En cualquier caso, y como una norma de inferior rango no puede ir en contra de una superior, debe entenderse que el acceso a esa información debe darse bajo las mismas garantías del artículo 15 de la Constitución Política, y los artículos 14 y 244 del Código de Procedimiento Penal, es decir, solo en casos de investigación penal, por medio de orden de la Fiscalía y bajo control judicial previo.

Además, la garantía constitucional de que el acceso a información de comunicaciones en Colombia sea exclusivamente por jueces o fiscales tampoco es suficiente. Es necesario que tanto las autoridades como los operadores implementen la presentación de informes de transparencia por parte de los actores involucrados para publicar información sobre quienes acceden a qué información y bajo qué justificación. Esto puede partir de la misma Resolución 3128 de 2011 que indica que es obligación del administrador de la BDA "disponer de mecanismos que permitan tener trazas de auditoría completas y automáticas relacionadas con el acceso a la BDA y las actividades de actualización o manipulación de la información".[40] Como todos los elementos del sistema, esto también debería estar detallado en la ley, pues afecta los derechos a la intimidad y a la libertad de expresión.

---

[38] Ley 1341 de 30 de julio de 2009, artículo 4, numerales 1 y 10.

[39] Código de Procedimiento Penal, artículo 244.

[40] Resolución CRC 3128 de 7 de septiembre de 2011, artículo 4, numeral 13.

Escenarios problemáticos

La asociación del IMEI, IMSI y número celular con datos personales, junto con la facultad de acceso a esta información por parte de autoridades definidas de manera ambigua, puede resultar en graves violaciones a derechos humanos.

Existe tecnología que permite simular la existencia de torres de telefonía para que los celulares se conecten a este simulador y entreguen los datos que usualmente entregarían al operador. Estos simuladores son conocidos como *IMSI Catchers* y pueden extraer información como IMEI, IMSI y otros datos de las comunicaciones de voz y mensajes de texto.[41] Hay muchos tipos y tamaños de *IMSI Catchers*, pero la posibilidad que ofrecen de capturar el IMEI junto con la existencia de las bases de datos positivas, que cualquier autoridad puede acceder sin controles adecuados, implica que un aparato puede identificar a una persona y viceversa.

En Ucrania, durante las protestas de principios de 2014, las personas que participaron en una manifestación recibieron un mensaje de texto que decía: "Querido suscriptor, ha sido registrado como participante en un motín". Las compañías de teléfonos involucrada negaron haber facilitado información de sus clientes y ninguna autoridad se hizo responsable por el mensaje.[42] Esto pudo haberse conseguido con el uso de un *IMSI Catcher*.[43] En Colombia, con este sistema, las autoridades no solo podrían obtener los teléfonos de las personas reunidas en un determinado lugar, sino también sus nombres, cédulas y direcciones físicas, entre otros, justamente porque tienen acceso a una base de datos que relaciona los datos técnicos del celular con información personal de la persona.

Siempre que exista una base de datos existe el riesgo de que caiga en manos equivocadas o de que sirva para propósitos ilegales. Por ejemplo, el gobierno mexicano implementó un sistema similar al colombiano exigiendo el registro de cada celular junto con los datos de la persona propietaria. Hacia 2010 se confirmó que los datos que había recogido el sistema estaban a la venta.[44] El peligro había sido advertido por la Comisión Nacional de Derechos Humanos, cuyo presidente había señalado que la información de las personas podía caer en manos equivocadas.[45] A raíz de los abusos cometidos por diferentes actores del sistema en contra de la

41 Privacy International. (s.f.). *Phone Monitoring* [blog post]. Disponible en https://www.privacyinternational.org/node/76.

42 Grytsenko, O. y Walker, S. (2014, 21 de enero). Text Messages Warn Ukraine Protesters They are "Participants in mass riot". *The Guardian*. Disponible en https://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot.

43 Franceschi-Bicchierai, L. (2014, 21 de enero). Someone Sent a Mysterious Mass Text to Protesters in Kiev. *Mashable*. Disponible en http://mashable.com/2014/01/21/kiev-protesters-text-message/#OQ4.MKEgtPqt.

44 Flores, P. (2010, 4 de junio). A la venta los datos de celulares del Renaut en México. *Hipertextual*. Disponible en https://hipertextual.com/2010/06/a-la-venta-los-datos-de-celulares-del-renaut-en-mexico.

45 Ojeda, F. (2009, 28 de junio). Comisión Nacional de Derechos Humanos: el registro de celulares es peligroso. *Hipertextual*. Disponible en https://hipertextual.com/2009/06/comision-nacional-de-derechos-humanos-el-registro-de-celulares-es-peligroso.

ciudadanía, el Senado terminó el sistema[46] y solo 3 años después se notificó que se había destruido la totalidad de los datos recogidos.[47]

En el Reino Unido, por su parte, la base de datos de clientes de un operador móvil fue atacada después de que la clave de acceso de un empleado resultara comprometida. La información personal de millones de personas estuvo en riesgo de ser capturada por los atacantes y vendida a terceros.[48]

Los abusos ocurridos en Ucrania, México y Reino Unido, a los que se suman muchos más, pueden ocurrir en Colombia y prueban la gravedad de la existencia de este tipo de bases. Nuestro particular contexto de violencia impone la necesidad de estudiar con más cuidado la necesidad de crear sistemas que hacen uso intensivo de información personal y de comunicaciones, que tienen el potencial de afectar gravemente la intimidad y la libertad de expresión.

Problemas derivados del procedimiento de verificación de IMEI

Vigilancia de las comunicaciones

Para entender cómo se afecta la intimidad con el registro de celulares, no basta con mirar el sistema en sí mismo. Es necesario ubicarlo como una pieza más del rompecabezas de la vigilancia de las comunicaciones en Colombia.

Sin importar el medio por el que ocurran, en Colombia las comunicaciones solo pueden ser interceptadas cuando hay una ley que autorice hacerlo y un juez dé la orden para realizar la interceptación. Por el momento, el único caso de interceptación legal que hay en nuestra ley es el de la necesidad de conocer las comunicaciones de una o varias personas involucradas en una investigación penal. Para esto se requiere una orden de Fiscalía y la revisión que una juez hace posteriormente para asegurarse que todo el procedimiento se haya hecho respetando la ley.[49]

---

[46] Senado cancela el Renaut (2011, 29 de abril). *El Economista*. Disponible en http://eleconomista.com.mx/sociedad/2011/04/29/senado-cancela-renaut.

[47] Monroy, J. (2013, 12 de mayo). Concluyó la destrucción de datos del Renaut. *El Economista*. Disponible en http://eleconomista.com.mx/sociedad/2013/05/12/concluyo-destruccion-datos-renaut.

[48] McGoogan, C. y Swinford, S. (2016, 18 de noviembre). Three Mobile cyber hack: six million customers' private information at risk after employee login used to access database. *The Telegraph*. Disponible en http://www.telegraph.co.uk/news/2016/11/17/three-mobile-cyber-hack--six-million-customers-private-data-at-r/.

[49] Para ampliar la información sobre la vigilancia de las comunicaciones en Colombia, pueden consultarse los siguientes documentos: Cortés, C. (2014). *Vigilancia de las comunicaciones en Colombia*. Bogotá, Colombia: Dejusticia, 18; Rivera, J.C. y Rodríguez, K. (2015). *Vigilancia de las comunicaciones por la autoridad y protección de los derechos humanos en Colombia*. San Francisco, EEUU: Electronic Frontier Foundation; Castañeda, J.D. (2016). ¿Es legítima la retención de datos en Colombia?. Bogotá, Colombia: Fundación Karisma; Pérez, G. (2016). *Hacking Team: malware para la vigilancia en América Latina*. Santiago, Chile: Derechos Digitales.

Aparte de este caso, hay otros que deberían ser tratados con las mismas restricciones —especialmente, la necesidad de control judicial previo— tales como el "monitoreo del espectro electromagnético" que puede hacer las agencias de inteligencia y el uso de herramientas de hackeo por parte del Estado.[50]

Retención y acceso a la información de las comunicaciones celulares

La interceptación, el monitoreo del espectro y el hackeo[51] son restricciones al derecho fundamental a la intimidad de las comunicaciones que deben ser implementados de forma legal, y solo cuando sea necesario y proporcional para alcanzar un fin legítimo. Sin embargo, hay una restricción en particular que merece más atención por ser más afín al sistema de registro de celulares. Esta es la retención de datos que consiste en la obligación de los proveedores de comunicaciones en Colombia de guardar cierta información de quienes contratan sus servicios para que autoridades como la Fiscalía y las agencias de inteligencia puedan acceder a esa información. Las normas que regulan la retención de datos en Colombia son muy ambiguas, así que vale la pena tratar los casos por separado.

Investigación criminal[52]

La Fiscalía, cuando investiga hechos que pueden ser delito, cuenta dentro de sus permisos con la facultad de acceder a la siguiente información de las personas suscriptoras del servicio de telefonía celular:

- "[L]os datos del suscriptor, tales como identidad, dirección de facturación y tipo de conexión".
- "Información específica contenida en sus bases de datos, tal como sectores, coordenadas geográficas y potencia, entre otras, que contribuya a determinar la ubicación geográfica de" los celulares son el objetivo de la investigación.

---

[50] Véase *Ley de actividades de inteligencia y contrainteligencia*. Ley 1621 de 17 de abril de 2013, artículo 17; y Fundación Karisma. (2016, 15 de noviembre). *ONU realiza observaciones frente a la privacidad, vigilancia y derechos humanos en Colombia* [blog]. Disponible en https://karisma.org.co/onu-realiza-observaciones-frente-a-la-privacidad-vigilancia-y-derechos-humanos-en-colombia/.

[51] *Hackear,* entendido como acceso intrusivo a sistemas, es una expresión que identifica una ética que consiste en propiciar el acceso a la tecnología para empoderar a las personas. Posteriormente, se entendió como la actividad de encontrar vulnerabilidades en sistemas de información con la idea de reportarlas y repararlas. Finalmente, se empezó a usar en el sentido de buscar vulnerabilidades en sistemas de información y aprovecharlas en forma ilícita. Para Karisma, la expresión correcta es *crackear*, por lo que utilizar la expresión *hackear* en ese sentido es incorrecta. Sin embargo, este no ha sido el uso que se ha popularizado. Para facilitar la comprensión del documento, hemos decidido usar el término *hackear* en el sentido de *crackear*, aunque somos conscientes de que es solo uno de los sentidos de esa palabra.

[52] Decreto 1704 de 15 de agosto de 2012.

Inteligencia[53]

La Ley de inteligencia permite que este tipo de agencias soliciten a los proveedores de servicios de telecomunicaciones la siguiente información sobre sus clientes:

- "[E]l historial de comunicaciones de los abonados telefónicos vinculados";
- "[L]os datos técnicos de identificación de los suscriptores [sic] sobre los que recae la operación"; y
- "[L]a localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización".

Las expresiones "datos del suscriptor" [sic] o "datos técnicos de identificación del suscriptor" [sic] e "historial de comunicaciones" no están claramente definidas en la ley. La Corte Constitucional, al hacer la revisión previa de esta ley, no dijo nada al respecto.[54] Sin embargo, el sistema de registro de celulares, especialmente todo lo que tiene que ver con los datos usados en el proceso de verificación, si se ven como un sistema legal –como un todo–, puede llenar ese vacío.

En adelante, cuando la Fiscalía o las agencias de inteligencia soliciten el acceso a los "datos del suscriptor" [sic] o a su "historial de comunicaciones" saben que los operadores están obligados a recopilar los metadatos asociados al registro de celulares y, en consecuencia, ya no bastará un par de datos, sino que será toda esta información a la que pedirán acceso. Mientras tanto, las reglas que aplican al acceso a esa información no son tan específicas y nunca fueron discutidas sobre esa base. Es decir, no se analizó el nivel en que el acceso a ellas puede ser violatorio de los derechos de las personas.

En otras palabras, sin las modificaciones a la Resolución 3128 de 2011 que hablan de los CDR, aún no sabríamos qué puede pedir inteligencia cuando hace uso de esa facultad de pedir los "datos técnicos del suscriptor" [sic] e "historial de comunicaciones". Como los operadores celulares ya deben recoger esa información por orden de la CRC y para efectos del sistema de registro de celulares, no sería extraño pensar que es esa misma información, y aún otra, la que piden estas agencias en uso de esa facultad. El problema es que una ley, aprobada en el Congreso después de los debates necesarios, es el único instrumento que puede decir a qué información de las comunicaciones pueden acceder las autoridades, no una resolución.

Al momento de estudiar la constitucionalidad de la Ley de inteligencia, la Corte Constitucional no tuvo en cuenta que era posible para los operadores generar toda la información que hoy deben reunir para cumplir con la regulación sobre hurto de celulares. Tampoco consideró que podrían centralizarla, de modo que, no solo se trata de la información que producen los celulares y almacenan los operadores,

---

[53] Ley 1621 de 17 de abril de 2013, artículo 44.

[54] Corte Constitucional. (2012). Sentencia C-540. M.P. Jorge Iván Palacio Palacio. Disponible en http://www.corte-constitucional.gov.co/relatoria/2012/C-540-12.htm.

sino de la información que produce una persona propietaria de uno o varios celulares, y los que conectan con la persona y que almacenan todos los operadores del país. Si se discutiera la obligación de retención de datos teniendo en cuenta toda la información que deben recopilar los operadores para el sistema de registro de celulares en Colombia, se vería lo extremadamente sensible que resultan los metadatos de las comunicaciones. Si esto hubiera formado parte de la evaluación, la decisión de la Corte Constitucional seguramente habría sido otra.

La ausencia de esta evaluación y de sus conclusiones, de ninguna manera puede suponer que las autoridades pueden acceder a esta información sin cumplir los requisitos del artículo 15 de la Constitución Política, es decir, que una ley permita la interceptación y que un juez dé la orden. En este caso, la ley que permite el acceso a la comunicación, o a los datos sobre ella, no es suficiente porque no es clara respecto a qué tipo de datos afecta. Tampoco menciona la necesidad de pedir autorización a un juez para acceder a la información. Es decir, no cumple el requisito de legalidad.

Metadatos de las comunicaciones: recopilación y entrega de CDR

Aunque hay principalmente dos tipos de comunicación que puede establecer un celular con la red —voz y datos— la regulación no es clara sobre los datos que deben entregarse para cada caso. Sin embargo, los datos de tráfico, dentro de que los caben los exigidos por la CRC, están definidos como toda

> *[P]ieza de información tratada a efectos de la conducción de una comunicación o de la facturación de la misma. Dentro de esta clase de datos se encuentran, entre otros, los datos necesarios para identificar el origen de una comunicación, el destino de la misma, la fecha, la hora, la duración de la comunicación y el tipo de comunicación.*[55]

Esta es información que, aunque no contiene nada sobre lo que se dice en la llamada o el mensaje, puede revelar mucho más que el contenido. Incluso más que la interceptación de la comunicación misma. Los metadatos "proporcionan una ventana a casi todas las acciones en la vida moderna, nuestros estados mentales, los intereses, las intenciones y los pensamientos más íntimos"[56], ya que están relacionados con el contexto y no con el contenido de la comunicación y hablan, entre otras cosas, de quién estuvo involucrado en la conversación, *cuándo, por cuánto*

[55] Resolución CRC 3066 de 18 de mayo de 2011, artículo 9.

[56] *Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones*. Disponible en https://necessaryandproportionate.org/es/necesarios-proporcionados#footnote3_l1wqc8l.

tiempo, con qué frecuencia, cómo, o a través de qué medios técnicos, desde dónde se hizo una llamada y dónde se recibió.[57]

Debido a la importancia que tienen estos datos respecto al derecho a la intimidad, la Corte Interamericana de Derechos Humanos ha dicho que este derecho protege el contenido de las comunicaciones, además de

> *[C]ualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones.*[58]

En la *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión* se ha señalado específicamente que la recolección y conservación de metadatos "equivalen a una limitación directa al derecho a la intimidad y vida privada de las personas". Una de las razones por las cuales es tan importante proteger adecuadamente esta información radica en su capacidad para revelar patrones, dar una idea del comportamiento de las personas[59], especialmente cuando se pueden cruzar y agregar varias fuentes de información.[60]

Como se ha dicho en varias ocasiones, es necesario considerar que la producción y retención de metadatos de las comunicaciones:

> *[A]umentan considerablemente el alcance de la vigilancia del Estado, y de este modo el alcance de las violaciones de los derechos humanos. Las bases de datos de comunicaciones se vuelven vulnerables al robo, el fraude y la revelación accidental.*[61]

---

[57] Loideain, N. (2015, 2 de junio). EU Law and Mass Internet Metadata Surveillance in the post-Snowden Era. Una versión revisada de este *paper* aparecerá en *Media and Communications*. *Special Issue on Surveillance: Critical Analysis and Current Challenges.* (2015). University of Cambridge Faculty of Law Research Paper No. 32/2015. Disponible en https://ssrn.com/abstract=2613424.

[58] Corte Interamericana de Derechos Humanos. (2009, 6 de julio). *Caso Escher y Otros vs. Brasil*. Disponible en http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf.

[59] El derecho a la privacidad en la era digital, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos: desde el punto de vista del derecho a la privacidad, "la agregación de la información comúnmente conocida como 'metadatos' puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada".

[60] Human Rights Council, *op. cit.* (nota 33), párr. 15.

[61] Ibíd., párr. 67.

Protecciones internas a las comunicaciones

Debido a la sensibilidad de los metadatos de las comunicaciones o CDR, el acceso a esta información por parte de una autoridad debe cumplir con los requisitos del artículo 15 de la Constitución. Estos requisitos son:[62]

1. Una ley que autorice el acceso
2. Un procedimiento establecido en la ley para realizar el acceso
3. Control judicial

Esto significa que las agencias de inteligencia no tienen en principio acceso a esta información, ya que no existe una ley que las autorice a interceptar comunicaciones, ni hay un procedimiento para hacer esa interceptación ni mucho menos control judicial. Para la Fiscalía, el acceso a los metadatos de las comunicaciones puede ser tratado como interceptación de comunicaciones, según los términos que usa la Constitución, o búsqueda selectiva en base de datos. En cualquier caso, se requiere orden del Fiscal en medio de una investigación penal y control judicial.

Adicionalmente, la Ley de protección de datos, especialmente sus principios, puede ser aplicada, ya que el IMEI es un dato personal. La CRC sostuvo, equivocadamente, que el IMEI no es un dato personal.[63] Alegó que en el registro no se solicita el número de la línea, pero olvidó que el artículo 7 de la Resolución 3128 de 2011 indica que la BDO positiva contendrá "la información correspondiente a IMEI-IMSI-MSISDN".[64] El número de la línea sí se involucra en el proceso y, por lo tanto, en los propios términos de la CRC, sí hay solicitud de datos personales. Sin embargo, no importaría que el número de la línea (MSISDN) no fuera solicitado. El IMEI es un dato personal porque el sistema de registro por diseño ha creado esa asociación entre IMEI e información personal (ver sección "Cada IMEI está atado a una persona"). La CRC había reconocido desde un principio que

[62] Corte Constitucional. (1993). Sentencia T-349. M.P. José Gregorio Hernández Galindo. Disponible en http://www.corteconstitucional.gov.co/relatoria/1993/T-349-93.htm.

[63] Concretamente, la CRC señala que "[e]s de precisar, que al solicitar la fecha y hora de la llamada asociada a los códigos IMSI, IMEI y al Código de Localización de Área (LAC) y Cell Identity (CI), no se están solicitando datos personales del usuario en los términos del literal c) del artículo 3 de la Ley 1581 de 2012, el cual determina que un dato personal "es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o [determinables]". En consecuencia, resulta evidente que al solicitar los referidos datos no es posible identificar la identidad y la ubicación del usuario que realiza la llamada, dado que no se requiere el MSISDN (número de la línea) puesto que conforme lo ha expuesto la Corte Constitucional es evidente que "la existencia de un dato personal se somete a la posibilidad de poder vincular una información concreta con una persona natural, específica o [determinable]". *Véase* CRC. (2015). *Fortalecimiento de BD*.

[64] Resolución CRC 3128 de 7 de septiembre de 2011, artículo 7, inciso 1.

> *En todo caso, teniendo en cuenta que la Base de Datos Negativa puede contener datos que eventualmente llegarían a identificar a un individuo, por tratarse del IMEI como pieza de información que de alguna manera se asocia a un propietario, bien sea persona natural o jurídica, el manejo de la información deberá observar lo dispuesto por la normatividad vigente en materia de protección de datos personales y la misma no podrá ser divulgada ni puesta en conocimiento de terceros no autorizados por las normas vigentes.*[65]

A pesar de esto, la CRC solicitó a la SIC un concepto sobre el tratamiento de la información contenida en los CDR, que incluye el IMEI. Según la SIC:

> *[E]l hecho de que un dato examinado aisladamente no logre identificar a priori a una persona, no implica, necesariamente, que no se pueda llegar a la individualización de la misma a partir del análisis de dicha pieza de información en conjunto con otros datos.*[66]

La SIC reconoce que el IMSI y el IMEI son números únicos. Por eso, "si la pieza de información de que se dispone se asocia con otro tipo de datos a los que se tiene acceso y de esta manera es posible individualizar a su titular", el tratamiento corresponde al de datos personales.[67] Según hemos explicado, las BD positivas asocian IMEI, IMSI y MSISDN con datos como el nombre, el número de identificación o la dirección.[68] Ahora bien, como se ha explicado, los metadatos pueden revelar información sobre las preferencias y hábitos de las personas. En este sentido, son datos sensibles.[69]

El tratamiento de los datos personales en las bases de datos y el del CDR o metadatos de las comunicaciones en la verificación, ordenado por la Resolución 3128 de 2011, violaría el principio de libertad del tratamiento de datos personales[70] y la prohibición expresa del tratamiento de estos datos[71], pues la excepción de trata-

---

[65] CRC. (2011). *Documento Soporte de la Resolución 3128 de 2011*. P. 19.

[66] Superintendencia de Industria y Comercio. (2016, 22 de enero)) *Concepto*. Radicado 16-1266-2-0.

[67] Superintendencia de Industria y Comercio (2016, 26 de enero). *Concepto*. Radicado 201630166, en CRC. (2016). *Revisión de las condiciones y criterios para la identificación de equipos terminales móviles: Etapa de verificación centralizada*.

[68] Resolución CRC 3128 de 7 de septiembre de 2011, artículo 7.

[69] Sobre los datos sensibles, la Corte Constitucional dice que en caso distinto se predica de la información sensible, relacionada, entre otros aspectos, con la orientación sexual, los hábitos del individuo y el credo religioso y político. En estos eventos, la naturaleza de esos datos pertenece al núcleo esencial del derecho a la intimidad, entendido como aquella "esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que al ser considerado un elemento esencial del ser, se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico". Corte Constitucional. (2008). Sentencia C-1011. M.P. Jaime Córdoba Triviño. Disponible en http://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm.

[70] *Ley de protección de datos personales*. Ley Estatutaria 1581 de 17 de octubre de 2012, artículo 4, literal c.

[71] Ibíd., artículo 6, inciso 1.

miento que constituyen no cumple con el requisitos de estar ordenado por una ley formal en reemplazo del consentimiento del titular.[72] En ese sentido, es necesaria la aplicación estricta de la obligación que pesa sobre el ABD para garantizar que los datos que administra no sean usados para fines distintos a los que pretende el sistema.[73] Sin embargo, por causa del diseño institucional del sistema, la vigilancia de este tipo de obligaciones no es sencilla. (ver sección “El sistema está en manos de terceros”).

Finalmente, la CRC ha decidido unilateralmente concederse acceso a los metadatos de las comunicaciones de todos las personas usuarias de telefonía celular en Colombia, pues exige a los operadores que entreguen, por cada llamada, IMEI, IMSI, fecha y hora de inicio y fin, y ubicación de inicio y fin.[74] Esto implica que una entidad cuya naturaleza es velar por mantener las condiciones de competencia en el mercado de las telecomunicaciones tendrá acceso a información sobre la intimidad de las personas, sin autorización legal y sin control judicial. Si esta recopilación masiva de metadatos de las comunicaciones es muy discutible para casos de investigación criminal e inteligencia, el acceso a los CDR o metadatos de las comunicaciones que exige la CRC es manifiestamente inconstitucional e ilegal.[75]

Durante el proceso regulatorio, el operador Claro manifestó que no había ejemplos de aplicación de un procedimiento de verificación en otros países. La CRC contestó que en el mundo había muy buenos ejemplos: Turquía, Egipto, Jordania, Ucrania, Azerbaiyán y Brasil.[76] Sobre los ejemplos, notó el operador Tigo que “no hay suficiente información nacional e internacional para adoptar medidas de control contra duplicados” y que las experiencias de las que se quiera tomar ejemplo “debe[n] guardar [relación] con el modelo constitucional del Estado”.[77] En otras palabras, lo que señala Tigo es que los estándares constitucionales de los países que la CRC pone como ejemplo son mucho menos garantistas que los colombianos.

Por ejemplo, Azerbaiyán se ha destacado por la persecución de personas críticas del gobierno, abogados y medios de comunicación, lo que le ha valido la condena de la Asamblea Parlamentaria y el Comisionado de Derechos Humanos del Consejo de Europa.[78] Además, la independencia del órgano regulador de tele-

---

[72] Ibíd. La *Ley de protección de datos personales* prohíbe el tratamiento de datos sensibles, “excepto cuando: a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización; […].”

[73] Resolución CRC 3128 de 7 de septiembre 2011, artículo 4.12.

[74] Ibíd., artículo 10.a.9, literales b y d.

[75] Ibíd.

[76] CRC. (2015). *Fortalecimiento de las bases de datos dentro de la estrategia nacional contra el hurto de equipos terminales móviles. Documento de respuesta a comentarios.*

[77] Tigo. (2016, 10 de marzo). *Comentarios proyecto regulatorio “Revisión de las condiciones y criterios para la identificación de equipos terminales móviles: etapa de verificación centralizada”.*

[78] Human Rights Watch. (2016). *World Report 2016. Azerbaiyán.* Disponible en https://www.hrw.org/world-report/2016/country-chapters/azerbaijan.

comunicaciones es dudosa y tiene un mercado móvil concentrado y con fuerte participación estatal.[79]

En Turquía se han denunciado los ataques oficiales contra la libertad de expresión y asociación. Durante el 2015, este país fue responsable de al menos tres cuartas partes de las solicitudes de bloqueo de trinos y cuentas en Twitter. En el mismo año, se permitió a la Dirección de Comunicaciones bloquear contenidos en internet.[80]

En Jordania se arrestó a un profesor universitario por hacer críticas en Facebook contra la cooperación de su país con Israel y se condenó a otra persona a 18 meses de cárcel por criticar a los Emiratos Árabes Unidos por el mismo medio.[81] Jordania también ha implementado otras medidas desproporcionadas como bloquear en todo el país el acceso a WhatsApp, Viber e Instagram por unas horas para evitar que un grupo de estudiantes de colegio hicieran trampa en los exámenes de fin de año.[82]

Egipto, por su parte, ha encarcelado a miles de personas pertenecientes al grupo de oposición más grande. Además, ha presionado a grupos de la sociedad civil a través de la solicitud de registros y de la revelación de información financiera.[83] La infraestructura de internet está controlada por el Gobierno, lo que le ha servido en el pasado para suspender u obstaculizar el acceso a internet.[84]

Claramente, los ejemplos de experiencias internacionales que cita la CRC para apoyar el procedimiento de verificación son incompatibles con las aspiraciones que surgen de la Constitución colombiana. Los párrafos anteriores evidencian la necesidad de eliminar el procedimiento de verificación y de tomar en cuenta el contexto de derechos humanos al momento de buscar ejemplos internacionales. El hecho de que países con violaciones graves a derechos humanos sean los únicos con un sistema como el colombiano debería ser suficiente para atender mejor a quienes, como Tigo, sugieren que el sistema no se ajusta a nuestro marco constitucional.

---

[79] Freedom House. (2016). *Freedom of the Net Report, 2016. Azerbaiyán*. Disponible en: https://freedomhouse.org/report/freedom-net/2016/azerbaijan.

[80] Human Rights Watch. (2016). *World Report 2016. Turquía*. Disponible en https://www.hrw.org/world-report/2016/country-chapters/turkey.

[81] Human Rights Watch. (2016). *World Report 2016. Jordania.* Disponible en https://www.hrw.org/world-report/2016/country-chapters/jordan.

[82] Freedom House. (2016). *Freedom of the Net Report, 2016. Jordania*. Disponible en https://freedomhouse.org/report/freedom-net/2016/jordan.

[83] Human Rights Watch. (2016). *World Report 2016. Egipto*. Disponible en https://www.hrw.org/world-report/2016/country-chapters/egypt#4023f5.

[84] Freedom House. (2016). *Freedom of the Net Report, 2016. Egipto*. Disponible en https://freedomhouse.org/report/freedom-net/2016/egypt#a1-obstacles.

Problemas del sistema en general

El sistema está en manos de terceros

Otro grave problema del sistema de registro de celulares en Colombia es que está diseñado de manera tal que la responsabilidad del sistema recae en un tercero, cuya relación está determinada por un contrato con los operadores, por tanto, no está sometido a los mismos controles que las entidades públicas. De ahí que haya menos transparencia y control democrático.

Según la Ley 1453 de 201185 y el Decreto 1630 de 2011[86], los operadores deben contratar con un tercero la administración de la BDA. En otras palabras, estas normas no solo crean las bases de datos, sino que ordenan a los operadores contratar con un tercero la creación y administración de la BDA. El proceso de verificación es aún más vago, pues a diferencia de lo que pasa con las bases de datos, no hay una orden para contratar con un tercero su administración y se habla en abstracto del "proceso de detección".[87]

El efecto más importante de este diseño es la falta de control y transparencia respecto a la forma en la que se centralizan las bases de datos. Por ejemplo, no hay una lista de condiciones para la contratación del tercero, lo que significa que los operadores no tienen que pensar, en principio, en privacidad y seguridad de las bases de datos. El decreto era el instrumento adecuado para fijar una lista de mínimos relacionados con el interés público que debe cumplir quien se encargue de la BDA, pero esto no se hizo. Las condiciones que debe cumplir El Corte Inglés, empresa encargada de la base de datos, están fijadas por medio de un contrato entre BDA y los operadores. Dado que es un acuerdo entre privados, ni la CRC ni el Ministerio TIC tiene acceso a ese contrato.[88] Sobre las condiciones del contrato que desarrollará el sistema de verificación, no hay información.

---

[85] El artículo 106 de la ley establece que "las bases de datos de que trata el presente numeral, deberán ser implementadas y administrativas [sic] de manera centralizada, **a través de un tercero**, por parte de los proveedores de redes y servicios de comunicaciones" [negrillas nuestras]. Ley 1453 de 24 de junio de 2011, artículo 106.

[86] El artículo 5 señala que la "obligación de implementación de las bases de datos. Los PRSTM deberán realizar la contratación y asumir los costos de implementación, administración, operación y mantenimiento de un sistema centralizado que soporte las bases de datos positiva y negativa, el cual deberá ser administrado por una persona jurídica independiente". Decreto 1630 de 19 de mayo de 2011, artículo 5.

[87] *Véase*, por ejemplo, lo que señala el artículo 10.b.2.iii: "El día tres y cuatro, los PRSTM identificarán los CDR de los IMEI que fueron remitidos de acuerdo con las condiciones del literal anterior y enviarán la información de los respectivos CDR al proceso de detección de IMEI duplicados entre las redes móviles de los PRSTM". Resolución CRC 3128 de 7 de mayo 2011.

[88] La CRC ha señalado que *"[l]a contratación del Administrador de la Base de Datos Administrativa corresponde a un proceso adelantado por los proveedores de redes y servicios de telecomunicaciones móviles con un tercero por ellos seleccionado, y se adelantó bajo el régimen de contratación privada, en cumplimiento de lo dispuesto en la Ley 1453 de 2011, el Decreto 1630 de 2011 y la Resolución CRC 3128 de 2011. En este sentido se informa que la Comisión no tiene copias de dicho contrato".* CRC. (2016, 12 de octubre). *Respuesta a solicitud de información*. Radicado 201671862.

Si el contrato no es conocido por ninguna autoridad, claramente, ninguna está controlando el desarrollo del sistema de registro, a pesar de las facultades amplias de intervención del Estado en las telecomunicaciones y de las facultades específicas del Ministerio TIC y la CRC.[89]

Por otro lado, la CRC regula un tema que es ajeno a su esencia. La esencia de la CRC es regulación para la eficiencia y calidad del sector. Dice la ley que creó la entidad que:

> *La Comisión de Regulación de Comunicaciones es el órgano encargado de promover la competencia, evitar el abuso de posición dominante y regular los mercados de las redes y los servicios de comunicaciones; con el fin que la prestación de los servicios sea económicamente eficiente, y refleje altos niveles de calidad.*[90]

Forzadamente, la Ley 1453 de 2011 asigna la función de regular el sistema a la CRC, cuando su propósito es reducir y desincentivar el hurto, asunto que no tiene directa relación con el propósito de la CRC. Esto puede explicar el hecho de que al sistema se ha añadido la función de controlar que solo los celulares homologados accedan a la red. Este caso no tiene relación alguna con el robo de celulares, pues la homologación consiste en verificar que los celulares cumplan con ciertas normas técnicas para seguridad de las personas y de la red.[91] En este caso, el sistema de registro trata un celular no homologado igual que uno robado, lo que tampoco tiene justificación y resalta la ambigüedad de las funciones de la CRC como entidad reguladora del proceso, así como el hecho de que el sistema puede recibir tareas que no pertenecen a su diseño original.

No puede ser la única solución

Hay que tener en cuenta otras medidas para combatir el hurto de celulares. El sistema no puede estar diseñado como si fuera la única solución. Esta pretensión es evidente en varios aspectos del diseño del sistema, por ejemplo:

- La unión de datos personales con IMEI y la comprobación de identidad.
- La creación de un procedimiento de verificación no previsto en la ley o el decreto.

[89] Ley 1341 de 30 de julio 2009, artículo 4.

[90] Ibid, artículo 19 inciso 2.

[91] Resolución CRC 087 de 15 de septiembre de 1997, Título XIII, Capítulo I.

- El nivel de detalle con el que se pretende controlar todas las posibilidades de duplicación de IMEI y la de los celulares no homologados, asunto que no tiene que ver con el robo de celulares.
- El hecho de que también pretenda hacer registrar los celulares perdidos, cuando esto no tiene que ver con el hurto. Un celular perdido no tendría por qué terminar siendo inútil. El sistema no puede pretender que cada celular funcione solo para su dueño.

En el Documento Soporte de la Resolución 3128, la CRC afirma que a pesar de los controles establecidos por los operadores contra el robo de celulares, especialmente la "lista negra", esta no es una

> *[H]erramienta completa y/o suficiente para frenar el hurto de Equipos Terminales Móviles —ETM—, ya que existe un mercado ilegal de dichos equipos, a los cuales se les ha alterado o duplicado el IMEI, siendo esta situación totalmente inadvertida en el proceso de autenticación del equipo en la red móvil.*

Si hay conciencia de que el sistema no puede ser la única solución, no debería ampliarse para buscar que cubra todas las aristas del problema. El sistema tiene que ser efectivo en lo que hace, pero no puede diseñarse como si fuera la única estrategia para afrontar el problema del robo de celulares.

El sistema no puede dar cuenta del cien por ciento de los celulares del país ni de todos los robos. Esto cobra importancia si se tiene en cuenta que esta medida no es efectiva cuando es posible cambiar el IMEI fácilmente[92] y los celulares son robados para ser vendidos por piezas.[93] Si, como se lo propone el sistema, la totalidad de los celulares que funcionan en Colombia son los celulares registrados y homologados y no hay ningún celular con IMEI duplicado en funcionamiento, aún habría motivos para robar un celular ya que puede servir por piezas. Si la medida no es efectiva para todos los casos de robo, no se justifica la constante ampliación del sistema, su pretensión de totalidad y la afectación a derechos fundamentales que significa.

El registro de celulares no se justifica ni siquiera en caso de que fuera efectivo, puesto que su principal problema es que afecta derechos fundamentales más allá de lo necesario para alcanzar sus objetivos. Es tanto como evitar las muertes por accidentes automovilísticos causados por borrachos en las noches bogotanas im-

---

92 Peñarredonda, J.L. (2015, 21 de abril). El cambio de IMEI y los repuestos: los ases tapados de los ladrones. *Enter.co*. Disponible en http://www.enter.co/cultura-digital/colombia-digital/el-cambio-de-imei-y-los-repuestos-los-ases-tapados-de-los-ladrones/.

93 Policía alerta por mercado de partes de celulares robados. (2016, 24 de febrero) *El Tiempo*,. Disponible en http://www.eltiempo.com/bogota/alerta-por-celulares-robados/16518588.

poniendo toque de queda a las 7 de la noche. La restricción a las libertades de las personas es tal que no se justifica siquiera con la importante disminución de muertes. La medida debe ser proporcional.

En todo caso, las cifras oficiales tampoco sugieren una disminución en el robo de celulares.[94] En Bogotá, la cifra de hurto se ha mantenido estable desde 2012, entre 9 y 11 mil reportes. La cifra más baja es de 2011, fecha en la que inició el sistema de registro de celulares, con poco más de 5 mil casos.[95] Estas cifras son simplemente indicativas de que el sistema probablemente no ha tenido grandes avances en la consecución de su objetivo. Sin embargo, son solo indicativas, pues sin variaciones sustanciales, aún si el sistema fuera efectivo, afecta injustificadamente los derechos a la intimidad y a la libertad de expresión.

La BD positiva y el proceso de verificación no sirven para combatir el hurto

La BD positiva registra todos los IMEI autorizados a funcionar. Aunque no está plenamente justificada por la CRC, si esta base tuviera alguna utilidad sería la de solo permitir el acceso a la red a los celulares con IMEI original o legítimo. En ese sentido, la base de datos positiva permite al sistema saber cuáles son los celulares que sí pueden operar, excluyendo el IMEI adulterado y haciendo efectiva la medida de bloqueo.

Sin embargo, este esquema presenta una nueva complicación: el IMEI de un celular robado puede cambiarse al de un celular autorizado para funcionar. Es decir, los IMEI de la lista positiva se podrían duplicar o clonar. En este caso, el sistema no sabe cuál es el celular legítimo y deja que ambos funcionen porque se identifican con un mismo IMEI autorizado. Esto implica que la base de datos positiva aún no hace que el sistema sea eficaz. Por esa razón existe el proceso de verificación ya explicado.

Como se vio, la idea del proceso de verificación es encontrar los IMEI duplicados e irregulares para que no funcionen en la red a través de la detección de los IMEI que han tenido actividad en la red diariamente. Este añadido tampoco es eficaz, porque si un IMEI puede cambiarse una vez, puede cambiarse varias veces. Si el nuevo IMEI adulterado es irregular porque, por ejemplo, no tiene la longitud estándar o porque tiene caracteres inválidos, el sistema lo bloqueará definitivamente. Sin embargo, si es un IMEI duplicado, la persona usuaria del celular legítimo tiene el deber de probar su condición bajo la pena de que el aparato resulte bloqueado. Tanto quien tiene un celular robado como quien tiene el celular legítimo y no puede probar esa situación pueden cambiar el IMEI si quieren que el celular

---

[94] El Sistema de información estadístico delincuencial, contravencional y operativo de la Policía (SIEDCO) reportaba más de 32 mil robos para 2011. Esta cifra ha aumentado hasta llegar a más de 52 mil casos en 2015.

[95] Roa, L. (2016). Extinción de dominio como herramienta contra el hurto de celulares en la ciudad de bogotá. *Revista Criminalidad*, 58 (2): 157-174. Disponible en http://www.scielo.org.co/pdf/crim/v58n2/v58n2a06.pdf.

siga funcionando, por lo que el sistema podría incentivar el problema que quiere combatir, que es la duplicación o adulteración de IMEI.

Puede argumentarse que adulterar un IMEI no es tarea fácil, por lo que detectar estos casos sí es eficaz. Sin embargo, si no es tan fácil, no es claro por qué es un problema que amerita medidas tan exageradas.

Según se señala en los informes de los operadores y la CRC, solo entre un 0,5 y 2% de los IMEI con actividad en sus redes son duplicados.[96] Aún si se estimara que el problema asciende a un 10% de los celulares con actividad en la red, el monitoreo constante de las comunicaciones de más de 52 millones de celulares no guarda proporción con el objetivo de la medida, aún más si se tiene en cuenta que no hay forma técnica de evitar con toda seguridad que solo funcionen los IMEI autorizados. Mientras tanto, los operadores deben guardar y analizar los metadatos de nuestras comunicaciones y deben compartir parte de ellos con la CRC y un tercero, con los problemas explicados anteriormente.

Como demuestra la historia regulatoria de este sistema, agregar medidas de control más agresivas no resulta en un sistema más eficaz para combatir el hurto de celulares. En todo caso, aún si así lo fuera, la medida no estaría justificada.

[96] CRC. (2016). *Revisión de las condiciones y criterios para la identificación de equipos terminales móviles: etapa de verificación centralizada*. P. 5.

• Conclusiones •

El poder ejecutivo, en general, y la CRC y el Ministerio TIC, en particular, deben adoptar una perspectiva de derechos humanos al diseñar, regular y ejecutar políticas sobre tecnologías de comunicación. Esto obliga no solo a observar la ley de protección de datos, sino también los estándares internacionales e interamericanos de protección a los derechos a la intimidad y a libertad de expresión.

Desde esta perspectiva, es claro que el sistema de registro de IMEI en bases de datos y el procedimiento de verificación vulneran los derechos a la intimidad y a la libertad de expresión. La asociación de una identificación a cada celular, junto con la obligación de los operadores de producción y entrega de metadatos de comunicaciones, va más allá del objetivo de la política, que es desestimular el hurto de celulares. Por el contrario, se convierte en una forma de identificar personas a través de sus equipos electrónicos, sirviendo así a fines de vigilancia por fuera del marco constitucional. Esto se refuerza con la comprobación de la falta de controles a la producción y el acceso a la información.

El sistema no separa adecuadamente las medidas para desestimular el hurto (base de datos negativa) de la persecución de los distintos delitos en donde resultan involucrados celulares. Así, el acceso a la información de las bases de datos de IMEI y metadatos de comunicaciones debe estar mediado por autorización judicial y para fines de investigación criminal en medio de un proceso de tal naturaleza.

Por otra parte, el diseño institucional del sistema representa un obstáculo para la transparencia que debe garantizarse para vigilar el cumplimiento de la ley y la Constitución.

No es aceptable crear un sistema que puede ser abusado por falta de controles y que, al buscar proteger el derecho a la seguridad y a la propiedad termina afectando los derechos a la intimidad y a la libertad de expresión de forma injustificada. En ese sentido, el sistema de registro de celulares debe ser derogado.

Un sistema que ayude a combatir el problema de criminalidad alrededor de los teléfonos celulares que respete las garantías establecidas en la Constitución y los instrumentos internacionales e interamericanos para la protección de derechos humanos debería evitar que cada persona pueda ser identificada automáticamente a través del IMEI, IMSI, SIM Card o número de teléfono. Además, debe restringir el uso de los metadatos de las comunicaciones para la verificación de los

IMEI pues esta es información que tiene la misma protección que el contenido de las comunicaciones. En ese sentido, basta con que cada operador reciba el reporte voluntario de los celulares robados y lo comparta con los demás operadores, al tiempo que reciben y comparten esta lista negativa con la GSMA y con otros países. En esta lista negativa no habría más información que cada IMEI reportado.

Según lo expuesto, la implementación de una base de datos negativa compartida por todos los operadores y conectada con la base de datos negativa de la GSMA lograría los mismos resultados del sistema actual y resultaría menos costosa para las personas, a quienes termina trasladándose el costo de este sistema, al tiempo que evitaría la vulneración a los derechos fundamentales de las personas en el uso de la telefonía móvil. Este sistema estaría soportado en la Decisión Andina 786 de 24 de abril 2013 y es, en líneas generales, el mismo que funciona en otros países y que funcionaba antes de 2011.[97]

---

[97] El marco normativo de ese sistema era la Resolución CRT 1732 de 2007, artículo 107 y la Circular Única de la Superintendencia de Industria y Comercio, Título III, Capítulo 2, numeral 2.6.

• Recomendaciones •

El sistema de registro de celulares en Colombia es ilegal por las razones vistas anteriormente. Sin embargo, las normas que lo sustentan tienen presunción de legalidad, lo que significa que es necesario que un juez declare que son ilegales. Sin necesidad de intervención judicial, la CRC puede eliminar y modificar ciertas partes de la Resolución 3128 de 2011 mientras que el Ministerio TIC puede derogar el Decreto 1630 de 2011 y proponer al Congreso la derogatoria del artículo 106 de la Ley 1453 de 2011. En ese sentido, las siguientes recomendaciones se enfocan en lo que puede hacer cada entidad para minimizar los riesgos que representa el sistema.

A la Comisión de Regulación de Comunicaciones

La CRC no tiene más facultades en el diseño del sistema que las establecidas en la Ley 1453 de 2011 y en el Decreto 1630. Estas normas ya establecen los puntos más problemáticos del sistema como la existencia de las BD positivas, la centralización de esa información en manos de un tercero y el procedimiento de verificación. Sin embargo, muchos detalles del sistema pueden ser modificados por la CRC. En ese sentido, recomendamos a esta Comisión:

- Eliminar la facultad ambigua del artículo 9 de la Resolución 3128 de 2011 para el acceso de cualquier autoridad a la información consignada en las bases de datos. La nueva redacción debe considerar que el acceso a esa información debe ser autorizado por un juez de la República a solicitud de la Fiscalía General y como parte del desarrollo de una investigación criminal, según lo ordenan los artículos 15 y 250 de la Constitución.
- Derogar todas las normas relevantes sobre el procedimiento de verificación, puesto que hace uso de los metadatos de las comunicaciones, información protegida por el artículo 15 de la Constitución Política. En ese sentido, debe interpretar restringidamente el artículo 9 del Decreto 1630 de 2011 y, por tanto, eliminar la verificación a partir de metadatos y dejar que los operadores simplemente verifiquen los IMEI frente a las bases de datos.

- Derogar el artículo 10.a.9 de la Resolución 3128 de 2011 que le permite el acceso a la propia CRC a los metadatos de las comunicaciones. El acceso a esta información debe cumplir con los requisitos del artículo 15 de la Constitución, que no cumple la regulación.
- En el futuro, la CRC debe interpretar las normas del sistema y, en general, todas las normas relacionadas con la vigilancia de las comunicaciones en sentido restrictivo. Es decir, debe solicitar orden judicial previa para el acceso a la información de los CDR o metadatos de las comunicaciones celulares y de internet, en desarrollo de una investigación penal o una operación autorizada de inteligencia, con orden de Fiscalía.
- Eliminar la obligación de asociar el IMSI y el MSISDN al IMEI que trae el artículo 7 de la Resolución 3128 de 2011. Esta asociación no está ordenada por el Decreto 1630.
- Eliminar la obligación de asociar en la BD positiva el nombre, dirección y teléfono de la persona propietaria del celular al IMEI que trae el literal d del artículo 7a de la Resolución 3128 de 2011. El Decreto 1630 solo menciona número de identificación.
- Eliminar la obligación en cabeza de los operadores de validar la identidad de la persona mediante la consulta en el Archivo Nacional de Identificación de la Registraduría Nacional, centrales de riesgo crediticio o demás fuentes. Esta obligación no aparece en el Decreto 1630 de 2011.
- En todo caso, para hacer seguimiento al sistema la CRC debe solicitar el contrato celebrado entre los operadores y El Corte Inglés para la administración de la BDA y hacerlo público.
- Implementar medidas de control respecto a la actuación de terceros sobre la información que recopila el sistema. Especialmente, debe vigilar la actuación de El Corte Inglés como ABD y publicar informes donde dé cuenta del cumplimiento de las obligaciones que la norma le impone respecto a la protección de los datos de las personas usuarias.

Al Ministerio TIC

- Derogar el Decreto 1630 de 2011 en lo relacionado con las bases de datos y el procedimiento de verificación.
- Considerar el impacto en derechos humanos que tiene el desarrollo de políticas públicas sobre tecnología e implementar discusiones, tanto internas como públicas, donde se haga una evaluación específica de este impacto, de manera previa a la implementación de la política.

- Detener el proceso de promoción de registro de celulares por el riesgo que representa para el ejercicio del derecho a la intimidad y a la libertad de expresión.
- En uso de la iniciativa legislativa que le reconoce la Constitución, proponer la derogatoria del artículo 106 de la Ley 1453 que asigna la función de regulación del sistema de registro de celulares a la CRC.
- Fortalecer mecanismos menos lesivos para combatir el robo de celulares tales como la colaboración entre operadores para permitir el reporte voluntario y bloqueo de celulares o la persecución, dentro del marco constitucional y legal, de bandas criminales dedicadas al robo de celulares.
- Como cabeza del sector de las TIC, el Ministerio debe velar porque siempre que un privado gestione información de las personas en desarrollo de una iniciativa pública, como es el caso del sistema de registro de celulares, se establezcan mecanismos de control y vigilancia efectivos. La calidad de tercero no debería implicar la disminución de obligaciones de protección de las garantías legales y constitucionales.

A los operadores de telefonía móvil

- No responder a peticiones de autoridades sin evaluar la legitimidad de la petición. Esto es verificar que las solicitudes cumplen los requisitos constitucionales y legales para la interceptación de comunicaciones, provienen de una entidad autorizada para acceder a la información, manifiesta una justificación para el acceso y limita a lo estrictamente necesario la información solicitada. Las solicitudes que no cumplan con estos requisitos deben ser rechazadas.
- Publicar informes de transparencia sobre las peticiones en los que se presenten estadísticas en los cuales se detalle qué autoridad solicitó qué tipo de información, qué justificación ofreció y si la solicitud fue atendida o rechazada.
- Incorporar la preocupación por el respeto al marco de derechos humanos en las participaciones ante el regulador y el Gobierno, tal y como lo hizo Tigo al señalar los graves problemas constitucionales del procedimiento de verificación.[98]
- Analizar la posibilidad de llevar las críticas que formularon al sistema de registro de celulares, especialmente las que indican el riesgo para el ejercicio de derechos humanos, a otras instancias. En ese sentido es recomendable que analicen la posibilidad de presentar estas objeciones por vías judiciales y defender de esta forma los derechos fundamentales de sus suscriptores.

---

[98] Tigo, *op. cit.* (nota 79).

A la Autoridad de Protección de Datos

- Acompañar activamente estas iniciativas gubernamentales que hacen uso intensivo de datos personales para verificar el cumplimiento de la Ley de protección de datos. La participación de la Autoridad de Protección de Datos desde las etapas iniciales de diseño de la política puede ayudar a evitar riesgos para el derecho a la intimidad y el habeas data que son más difíciles de mitigar cuando la política ha sido avanzada.
- Considerar el desarrollo de un procedimiento como el establecido en la Resolución 44649 de 2010, ordenado por el Decreto 2897 de 2010, por medio del cual se identifican riesgos a la competencia de forma previa a la toma de decisiones regulatorias. En todo caso, el procedimiento de verificación previo no puede constituir un obstáculo para discutir y efectuar veeduría ciudadana sobre los temas de la evaluación previa.

Una publicación de:

Fundación Karisma

Con el apoyo de:

PRIVACY INTERNATIONAL